12th ICCRTS
"Adapting C2 to the 21st Century"

Frameworks and Insights Characterizing Trends in Cyberspace and Cyberpower

Track: C2 Concepts, Theory, and Policy

Franklin D. Kramer, Stuart H. Starr (Point of Contact), Larry Wentz, Elihu Zimet
Center for Technology and National Security Policy (CTNSP)
National Defense University (NDU)
Grant Hall, Fort Lesley J. McNair
Washington, DC 20319

Franklin D. Kramer: 202-685-3578; KramerF@ndu.edu
Stuart H. Starr: 202-685-2657; StarrS@ndu.edu
Larry Wentz: 202-685-3914; WentzL@ndu.edu
Elihu Zimet: 202-685-3586; ZimetE@ndu.edu

Daniel Kuehl
Information Resources Management College (IRMC)
National Defense University (NDU)
Marshall Hall, Fort Lesley J. McNair
Washington, DC 20319
Phone: 202-685-2257
KuehlD@ndu.edu

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Frameworks and Insights Characterizing Trends in Cyberspace and Cyberpower	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University (NDU),Center for Technology and National Security Policy (CTNSP),Grant Hall, Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Twelfth International Command and Control Research and Technology Symposium (12th ICCRTS), 19-21 June 2007, Newport, RI

14. ABSTRACT

During the course of the Department of Defense's (DoD) 2006 Quadrennial Defense Review, it was observed that DoD lacks a coherent, holistic framework to formulate and assess policy issues associated with cyberspace and cyberpower. To redress that shortfall, the Under Secretary of Defense (Policy) directed the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), to undertake a cyberpower study. As stated in the study's Terms of Reference, " there is a compelling need for a comprehensive, robust and articulate cyber power theory that describes, explains and predicts how our nation should best use cyber power in support of US national and security interests". Consistent with that goal, this paper addresses four issues. First, it provides a holistic framework for addressing cyberpower issues and it summarizes the major findings of several studies that are being developed to characterize that framework. Second, it identifies and discusses potential Measures of Merit (MoMs) that can be applied to layers of that holistic framework. Third, to illustrate the types of analyses that are being pursued, a framework for tactical Influence Operations is introduced and applied. The paper concludes with some broad observations on the nature of the cyberpower problem.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**34**	

Frameworks and Insights Characterizing Trends in Cyberspace and Cyberpower

Frank Kramer, Stuart Starr, Larry Wentz, Eli Zimet
Center for Technology and National Security Policy (CTNSP),
National Defense University (NDU)

Daniel Kuehl
Information Resources Management College (IRMC), NDU

Abstract

During the course of the Department of Defense's (DoD) 2006 Quadrennial Defense Review, it was observed that DoD lacks a coherent, holistic framework to formulate and assess policy issues associated with cyberspace and cyberpower. To redress that shortfall, the Under Secretary of Defense (Policy) directed the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), to undertake a cyberpower study. As stated in the study's Terms of Reference, "… there is a compelling need for a comprehensive, robust and articulate cyber power theory that describes, explains and predicts how our nation should best use cyber power in support of US national and security interests".

Consistent with that goal, this paper addresses four issues. First, it provides a holistic framework for addressing cyberpower issues and it summarizes the major findings of several studies that are being developed to characterize that framework. Second, it identifies and discusses potential Measures of Merit (MoMs) that can be applied to layers of that holistic framework. Third, to illustrate the types of analyses that are being pursued, a framework for tactical Influence Operations is introduced and applied. The paper concludes with some broad observations on the nature of the cyberpower problem.

A. INTRODUCTION

During the course of the Department of Defense's (DoD's) 2006 Quadrennial Defense Review (QDR)(Reference 1), it was observed that DoD lacks a coherent, holistic framework to formulate and assess policy issues associated with cyberspace and cyberpower. To redress that shortfall, the Under Secretary of Defense (Policy) directed the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), to undertake a study of the subject area. As stated in the study's Terms of Reference, "… there is a compelling need for a comprehensive, robust and articulate cyber power theory that describes, explains and predicts how our nation should best use cyber power in support of the United States (US) national and security interests".

In order to address these issues, a framework has been developed that can be depicted as a pyramid. In the framework, the foundation of the effort is established by characterizing key definitions (e.g., "cyberspace", "cyberpower", cyberstrategy) and exploring possible changes in cyberspace over the next 15 years. Building on that foundation, the next layer

of the framework explores the potential impact of changes in cyberspace on selected levers of power (i.e., military, informational). The third level of the pyramid addresses the extent to which changes in cyberspace serve to empower key entities. These entities include, *inter alia*, individuals, activists, terrorists, transnational criminals, nation states, and supra-national organizations (e.g., the United Nations (UN)). Another facet of the pyramid considers key factors that transcend each of these factors. These include institutional and policy issues that the community must address (e.g., governance, legal, government-corporate responsibilities).

Several workshops have been convened to address each of these areas. At these workshops, leading experts from government, think tanks, industry, and academia have presented their views on the major subject areas. Based on the feedback from those discussions, each presenter is developing a chapter for a comprehensive book on the subject.

This paper introduces selected frameworks for conceptualizing the problem, suggests a hierarchy of Measures of Merit (MoMs) to support policy analysis, discusses preliminary analyses that have been performed based on those frameworks, and identifies residual issues that warrant further research.

B. HOLISTIC FRAMEWORK

As a point of departure, a project framework has been developed that can be depicted as a pyramid (see Figure 1).

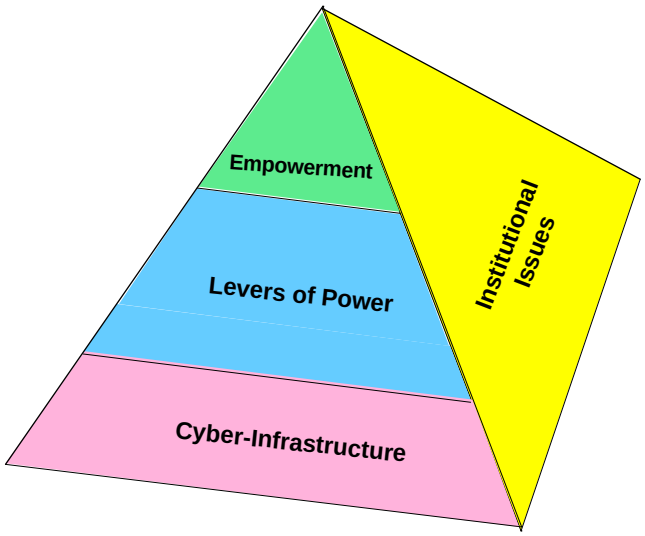


Figure 1. Holistic Framework for Cyberspace and Cyberpower

In the framework, the foundation of the effort is established by characterizing key definitions (e.g., ”cyberspace”, ”cyberpower”, “cyberstrategy”) and by exploring possible changes in cyberspace over the next fifteen years. This layer of the framework is typically characterized by Measures of Performance (MoPs) (e.g., connectivity, bandwidth, resistance to adversary actions). Building on that foundation, the next layer of the framework explores the potential impact of changes in cyberspace on selected levers of power (i.e., military, informational). This layer of the framework is typically characterized by Measures of Effectiveness (MoEs) (e.g., for military operations, changes in loss exchange ratios). The third level of the pyramid addresses the extent to which changes in cyberspace serve to empower key entities. These entities include, *inter alia*, individuals, activists, terrorists, transnational criminals, nation states, and supra-national organizations (e.g., the UN). This layer of the framework is typically characterized by Measures of Entity Empowerment (MoEEs) (e.g., the extent to which an entity can perform key functions and missions as a consequence of the capability afforded by changes in cyberspace). Another facet of the pyramid considers key factors that transcend each of these factors. These include institutional and policy issues that the community must address (e.g., governance, legal, government-corporate responsibilities).

1. Layer 1: Cyber-Infrastructure

At the bottom level of the pyramid, four white papers are being developed to clarify the dimensions of cyber-infrastructure.

In his white paper (Reference 2), Dan Kuehl has defined several key terms:
“**Cyberspace** is an operational domain characterized by the use of electronics and the electronic spectrum to create, store, modify, and exchange information via networked and interconnected information systems and telematic infrastructures.”
“ **Cyberpower** is the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power.”
“**Cyberstrategy** is the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power.”

To address projected evolutionary changes in cyberspace, two complementary chapters are being generated. The initial chapter, by Ed Skoudis (Reference 3), emphasizes many of the computer science dimensions of the problem (e.g., the transition from Internet Protocol (IP) version 4 to version 6; wireless proliferation, in the areas of wireless fidelity (WiFi) and Radio Frequency Identification Devices (RFID)). It focuses on likely increases in the capabilities and vulnerabilities of cyberspace. That chapter is complemented by a chapter by Eli Zimet that describes and discusses a set of domains of cyberspace (Reference 4) The elements of the domain include architecture (e.g., transport, services, applications), information content, and people (e.g., knowledge, culture, behavior). The cumulative result of these two chapters is to identify a range of cyber trends and cyber issues. These results are summarized in Tables 1 and 2, respectively.

Trends	Observations
Increased move to Internet Protocol (IP)	Convergence of telephony, radio/TV, and Internet (e.g., Voice over IP (VoIP), streaming video)
Merging of hardware and software	Fixed function devices
Sensor networks	Proliferation of heterogeneous sensors
Broadband and wireless proliferation	City-wide deployment of Worldwide Interoperability for Microwave Access (WiMax)
Enhanced search capabilities	Both Internet-wide and local-system
Enhanced human/machine connectivity	Direct nerve and brain connections to computer or prosthesis
Increased user participation in information content	Proliferation of web logs (blogs), Wikis
Increased information push	Complementing information pull

Table 1. Cyber Trends and Observations

Issues	Observations
Increased volume of traffic	Increased congestion and packet loss
Governance and control of the Internet	US vice global roles
Net neutrality	Internet service becomes a commodity
Security, vulnerability, robustness	Increasing concerns
International terrorism hosted in cyberspace	Increasing and disturbing trend
Research for future advancements	In computer science and network architectures

Table 2. Cyber Issues and Observations

In a subsequent white paper, Marjory Blumenthal and Dave Clark (Reference 5) identified and discussed potential revolutionary changes in cyberspace. They focused on three key factors. First, they identified potentially revolutionary changes in new computing. They foresee a decade of cheap, ubiquitous, low power computing. As one

manifestation, they envision the computerization of "everything" (e.g., proliferation of ubiquitous sensor networks). Second, they raise the question about investment in the Internet of the future. They observe that today, the Internet is an open platform. If Internet service becomes a commodity they worry about who would make the investments in the needed technology to keep it robust. Finally, they address the issue of security. They foresee two alternative futures. Consistent with current trends, they project continued erosion of trust and confidence in the Internet. Alternatively, they note the possibility of major corrections to the current situation. As one example, they cite the National Science Foundation's (NSF's) Future Internet Design (FIND) in which security and management would be designed in from the beginning and rapid topological reconfiguration would be possible. Alternatively, the Defense Advanced Projects Agency (DARPA) is contemplating beginning an Assurable Global Networking (AGN) initiative for the military's Global Information Grid (GIG), in which highest priority would be given to the features of assurability and support for mobility.

2. Layer 2 – Levers of Power

At the next level of the pyramid, four white papers are being generated. Greg Rattray (Reference 6) provides a historical perspective by assessing the common features of environmental power theories (e.g., Mahan on naval power; Douhet on airpower; Mackinder on land power; Gray and Sloan on space power). Based on those earlier efforts, he has identified five common features of environmental power theories: political-military impact of technological trends; pace and scope of operations; national mobilization of key resources; recognition of logistics and lines of communication (LOCs); and gaining control of key features. Table 3 summarizes the implications of these five common features for a theory of cyberpower and cites selected examples.

Common Features of Environmental Power Theories	Implications for a Theory of Cyberpower	Observations
Political-Military impact of technological trends	New realm for political dialogue and conflict	□Blogging □Terrorist use
Pace and scope of operations	Ever increasing speed	□Slammer worm □Video of beheadings
National mobilization of key resources	□Management of cyberspace as a joint economic/military domain □Centrality of human resources	□Contrasting approaches (e.g., US, China) □Locus of expertise in commercial sector
Recognition of logistics and Lines of Communications (LOCs)	□Physical □Logical	□Long haul, interconnection points □Logical standards/mgt of IP
Gaining control of key features	□Physical □Code/logical assets	□Undersea cables, satellites □Governance in a global community

Table 3. Common Features of Environmental Power Theory and Cyberpower

Martin Libicki (Reference 7) complements that perspective by exploring cyberspace and the modern military. He observes that enhancements in cyberspace promise substantial performance in air-to-air combat when aircraft are provided digital Link 16 information in addition to voice communications. For example, recent experiments demonstrate approximately a 2.6 times increase in Blue kill ratios due to the addition of Link 16 information. This increase can be ascribed to earlier, more complete shared situational awareness and understanding, more decision time available, better intercept geometries, and improved lethality of engagements (Reference 8). However, the advantages of enhancements in cyberspace for land operations are more difficult to quantify. A study of the Stryker Brigade Combat Team effectiveness at the Joint Readiness Training Center demonstrated improvements over a Light Infantry Brigade (Reference 9). However, it is difficult to ascribe the Stryker's enhanced effectiveness to improved connectivity due to differences in mobility, firepower, and time to conduct reconnaissance. Thus, this white paper concludes that networking helps, but more experimentation will be needed to assess quantitatively how much it helps.

The informational lever of power is being addressed at the strategic, operational, and tactical levels. At the strategic and operational levels, Frank Kramer and Larry Wentz (Reference 10) identify three key elements of influence operations: expertise in the application of principles of influence; domain experience in arenas where the principles are to be applied; and experience in the use of cyberspace. These factors demand improvements in education, training, and experience. At the tactical level, Stuart Starr (Reference 11) proposes a framework, based on the Mission Oriented Approach to assessment (Reference 12), to provide a logical way of organizing and addressing Influence Operations issues. Subsequently, he employs the DOTMLPF[1] paradigm to provide a systematic means of identifying shortfalls and addressing holistic packages of action. The results of those analyses are summarized in Section D of this paper.

3. Layer 3 – Empowerment of Key Entities

At the top of the pyramid, three white papers are being prepared to explore the extent to which cyberspace is empowering key entities.

Jarret Brachman (Reference 13) observes that new social movements are employing cyberspace to support twelve key functions: empower and catalyze corporate action; focus movement energy on pursuit of broader social change objectives; foster a favorable public image through targeted information campaigns; build and develop a coherent and compelling ideology; provide the movement with a variety of information and knowledge; make money, facilities, and other resources as widely available as possible; facilitate freedom of movement, expression, and action; offer protection to participants where possible; build and sustain movement morale and further cement solidarity; continuously recruit new participants; nurture new generations of leadership; and pragmatically forge external coalitions and treaties. In his white paper, he explores how militant Salafi terrorists are employing cyberspace to enhance their ability to perform all of these functions. In particular, he focuses on their use of cyberspace to empower action,

[1] Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities

focus on social change, foster public awareness, support comprehensive education, promulgate their ideology, cement solidarity, and nurture new leadership.

As context, Kevin Burton (Reference 14) identifies the priorities of the Federal Bureau of Investigation's (FBI's) Cyber Division: counterterrorism intrusions; counterintelligence intrusions; criminal intrusions; innocent images; intellectual property; and Internet fraud. Within that context, he identifies a broad set of activities that transnational criminals are employing to exploit cyberspace. These include phishing, identity theft, money/merchandise re-shipping (e.g., recruitment of "mules" via on-line job search sites), extortion (e.g., use of limited distributed denial of service attacks using botnets to threaten a victim), and intrusion (e.g., stealing data from competitors; mapping the network for future use). In the future, he foresees threats to key critical infrastructures (e.g., Supervisory Control and Data Acquisition (SCADA) attacks) and the compromise of Sensitive But Unclassified (SBU) networks.

Tim Thomas' white paper on nation-state empowerment (Reference 15) provides insights on the projected uses and cyber-strategies of China and Russia. He discusses the recent writings from key conceptual thinkers in those nations and compares and contrasts these strategies. He observes that these nations use a different vocabulary in discussing cyberspace and cyberpower. For example, Chinese writings on the subject focus on stratagems, objective and subjective reality, and the dialectic (i.e., "reasoning that juxtaposes opposed or contradictory ideas and seeks to resolve conflict"). He emphasizes two key aspects of the Chinese view of the Revolution in Military Affairs:
"War with the objective of expanding territory has basically withdrawn from the stage of history, and even war with the objective of fighting for natural resources is now giving way to war with the objective of controlling the flow of financial capital."
Furthermore:
"If we go our own path to develop military theory, weapons, and equipment, we will develop something never seen before in places that no one has ever thought of before; others will be unable to anticipate or resist our 'self-accommodating systems'".
As an illustration of "self-accommodating systems" against the superior foe, three ways are cited for making a cat eat a hot pepper: "stuff it down his throat, put it in cheese and make him swallow it, or grind it up and spread it on his back. The latter method makes the cat lick itself and receive the satisfaction of cleaning up. The cat is oblivious to the end goal. This is strategy."

4. Other Face of the Pyramid – Institutional Issues

Four white papers are being prepared which address key institutional issues. The white paper by Hal Kwalwasser (Reference 16), which is being developed in concert with Jody Westby, is focusing on the issues of governance and the Internet Governance Forum (IGF). The IGF is to be multi-lateral, multi-stakeholder, democratic, and transparent. The first IGF was held in Athens, Greece in October 2006. Although no decisions were taken at the Athens IGF, it served to articulate the general views of the participants. These include: little interest in changing the governance of the Internet Corporation for Assigned Names and Numbers (ICANN); even less interest in some new government-

focused governance structure; general concern over cyber security and spam; hostility toward censorship and controls; and concern about "fair use" of copyrighted material on the Internet. The next meeting of the IGF will be in Brazil in November 2007.

A white paper on Critical infrastructure Protection (CIP) is being developed by Will O'Neil (Reference 17) in concert with John McCarthy. As context, it is noted that connectivity of infrastructure networks generally adhere to power laws (e.g., scale free networks) versus exponential (or sparse) laws. Consequently, there tend to be a relatively small set of critical nodes that are richly connected. Although there are currently seventeen infrastructures that are characterized as "critical", electric power tends to be a particularly critical infrastructure. It poses macro-survivability issues because of its multiple "Achilles heels" (e.g., physical attack; SCADA attack), divided, overlapping regulatory responsibilities (e.g., Department of Homeland Security, Department of Energy, Federal Energy Regulatory Commission (FERC), states), and the potential for cascading effects to other critical infrastructures in the event of a failure. Although there has been a Congressionally-mandated study that highlighted the threat posed by Electromagnetic Pulse (EMP) attack to the electric power sector, it is observed that it would take an extremely sophisticated adversary to implement it. Overall, there is concern that the US lacks a coherent strategy to guide CIP efforts. In particular, there is a need for a framework to drive CIP investments, augmented with a clear, unambiguous taxonomy and lexicon.

A white paper on legal issues and cyberspace is being developed by Tom Wingfield (Reference 18). In view of the challenges posed by attack attribution in cyberspace, a key issue revolves around the question, "What constitutes an armed attack in cyberspace?" As a framework, the UN language provides a point of departure. This revolves around *jus ad bellum* (i.e., Article 39 ("threat to peace") and Article 2(4) ("threat/use of force")) and *jus in bello* (Article 51 ("armed attack")). For example, blockades designed to block creation of wealth constitute "armed attack". In the Information Age, efforts to block the flow of information, and thereby choke off the life-blood of a service economy, would constitute an armed attack. One of the major legal challenges is the application of *jus ad bellum* to computer network attack. One way of addressing that issue is to apply the Schmitt Analysis that explores seven factors that may make the action "look military" (severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility). Overall, a holistic, non-mechanical analysis of Article 2(4) would address the question "Have I been badly enough hurt to strike back?" In summary, the basic challenge is whether we require a new legal framework and associated basic principles for the issues of cyberspace and cyberpower.

A white paper on methods and tools to analyze cyberspace and cyberpower issues is being developed by Jim Kadtke (Reference 19). Preliminary insights suggest that exploratory analysis approaches will be needed to capture the broad dimensions of the response surfaces. Furthermore, a range of orchestrated techniques will be required that include, *inter alia,* expert elicitation, computational social science techniques (e.g., Senturion), influence diagrams (e.g., Situation Influence Assessment Module (SIAM)), system dynamics models (e.g., iThink), Colored Petri Nets (e.g., Pythia), virtual reality

tools (e.g., Second Life), and agent based models (e.g., Synthetic Environment for Analysis & Simulation (SEAS)). However, a broad range of challenging issues persist. For example, we know very little about the basic underlying science (e.g., complex adaptive systems) and our existing analytic tools are unable to address key issues adequately (e.g., we lack good representations of network behavior, particularly when the networks are subjected to malicious code).

C. MEASURES OF MERIT

This section of the paper will explore Measures of Merit (MoMs) for cyberspace and cyberpower. This section will begin by providing some contextual information. It then introduces four levels of MoMs: MoPs, Measures of Functional Performance (MoFPs), MoEs, and MoEEs.

1. Context

The Operations Research (OR) community has frequently sought to identify appropriate MoPs and MoEs to characterize national security issues. In the North Atlantic Treaty Organization (NATO) Code of Best Practice for Command and Control (C2) Assessment (Reference 20), MoMs were introduced that subsume MoPs and MoEs. They extended the range of measures by introducing the concept of Measures of Policy Effectiveness (MoPEs).

Building on that framework, the analytical community faces the following issues. First, how can the analyst characterize a set of subordinate measures? Second, how can the analyst derive a set of relationships to link those measures?

The following set of measures represents a preliminary attempt to identify MoMs that are useful in characterizing and linking measures for cyberspace and cyberpower
Since this field of endeavor is still in its infancy, the material is meant to be illustrative and not exhaustive.

2. Measures of Performance (MoPs)

Three types of MoPs may be employed to characterize cyberspace. First, a set of infrastructure MoPs are needed to characterize the key computer science and electrical engineering dimensions of the problem. A key measure is the amount of bandwidth that is available to representative users of cyberspace. As the bandwidth increases to the megahertz/sec range, the user is able to access advanced features such as imagery and video products. A second key measure is connectivity. For circumstances in which the cyber-infrastructure is fixed, a useful measure is the percent of people in a country that have access to the Internet. However, in many military operations, the cyber-infrastructure and the users are mobile. Under those circumstances, a more useful measure is the performance of Mobile, Ad hoc NETwork (MANET) users (e.g., their ability to stay connected). Third, one can introduce measures of the “noise” that characterizes the cyber-infrastructure. For example, the extent to which the quality of the

Internet is degraded can be characterized by the unwanted e-mail that it carries ("spam"), which can subsume a substantial subset of the network's capacity. As an example, it has been estimated that in recent months approximately 90% of the traffic on the Internet is spam (Reference 21). In addition, the integrity of the information is further compromised by "phishing" exploits in which criminal elements seek to employ the Internet to perpetrate economic scams. Finally, MoPs can be introduced to characterize resistance to adversary actions, including denial of service attacks, propagation of viruses or worms, and illicitly intruding into a system.

A second class of MoPs deals with the content of the information in cyberspace. As an example, representative measures could include the ability of users to locate and access information in cyberspace in a useful, timely manner. The issue of access is of specific concern to the military where different levels of classification pose a significant challenge.

The third class of MoPs addresses the ability of users to employ the information in cyberspace. As one facet of these measures, the user must be able to understand the information. This will be a function of the metadata that are provided. In addition, the user must be able to trust the information. To some degree, this will be a function of the pedigree of the information. The Assistant Secretary of Defense (Networks and Information Integration)'s (ASD(NII)'s) data initiative is intended to enhance the performance for each of these two classes of MoPs (Reference 22).

3. Measures of Functional Performance (MoFPs)

It is useful to introduce MoFPs that characterize how successfully selected entities are able to perform key functions, taking advantage of cyberspace.

As an illustration, terrorists are aggressively using cyberspace to enhance their ability to perform a number of key functions. These include their ability to attract recruits to their cause, raise funds to support their operations, disseminate their message to a world-wide audience, support training of recruits (since they have lost many of their physical training facilities), support distributed planning of operations, and implement command and control of selected operations.

In the case of the US military, the concept of net-centricity is to employ advances in cyberspace to perform essential functions. These include the ability to enhance the performance of increasing levels of information fusion (e.g., at level 1, the ability to generate a timely, complete, accurate picture of Blue forces). Similarly, a basic tenet of net-centricity is to propagate commander's intent so that the participants in the operation can synchronize and self-synchronize their actions.

4. Measures of Effectiveness (MoEs)

MoEs are needed to characterize how effective entities can be in their key missions, taking advantage of cyberspace. As an example, the MoEs for terrorists might

characterize their ability to successfully plan and execute their operations as measured by the number of casualties that they create and their disruption of the economy. Furthermore, MoEs are needed to assess their ability to terrorize the targeted population as measured by the extent to which they disrupt normal life (e.g., deter the populace from using commercial air travel).

In the context of Major Combat Operations, MoEs are needed to characterize the ability to exploit cyberspace in multiple dimensions. At one extreme, enhancements in cyberspace have the potential to reduce the time to conduct a campaign and the casualties associated with the campaign. At the other extreme, enhancements in cyberspace may substantially enhance Blue loss exchange ratios and the amount of ground gained and controlled. There is also a need to generate comparable MoEs for Stabilization and Reconstruction Operations (SRO). In a recent paper, it is maintained that "I-Power" (i.e., the effective use of information and communications technology) can be an effective enabler of other key reconstruction activities (e.g., education, medical) (Reference 23).

5. Measures of Entity Empowerment (MoEEs)

From the perspective of cyberpower, there is interest is characterizing the extent to which enhancements in cyberspace can empower key entities. As an illustration, observe that for an individual, features of cyberspace (e.g., the proliferation of blogs and wikipedias) enable the individual to exert greater influence over a range of national security events (e.g., elections, passage of legislation, public opinion on national security). Similarly, activists are able to leverage cyberspace to attract supporters to their cause. This includes support for treaties (e.g., recent efforts to ban landmines) and support for a disadvantaged group (e.g., public support for the Zapatistas in Mexico).

In the case of Islamic fundamentalist terrorists, they seek empowerment in two key areas. First, they have espoused a range of geo-political goals (e.g., expel westerners from bases in the Middle East; reinstitute the caliphate; change constitutions to implement Sharia law). In addition, they are attempting to generate favorable "Economic Exchange Ratios" for their operations. As an example, the incidents of 9-11 entailed costs on the order of hundreds of thousands of dollars for the terrorists and resulted in losses on the order of hundreds of billions of dollars to the US economy.

Finally, in the case of nation states, potential MoEEs might include the ability to leverage cyberspace to influence a population (e.g., "win hearts and minds"), shape a nation at strategic crossroads, and deter, persuade, and coerce an adversary.

6. Observations on MoMs

This discussion suggests that a family of MoMs will be needed to characterize cyberspace and cyberpower. It must be emphasized that the examples cited are meant to be illustrative. The next steps will entail refining the taxonomy of measures, developing a more complete set of measures, and beginning to develop relationships that link these measures.

D. TACTICAL INFLUENCE OPERATIONS – AN EXAMPLE

The objectives of this section of the paper are two-fold. First, it introduces a framework for characterizing and ameliorating key shortfalls associated with Influence Operations. It then illustrates the framework by applying it to a tactical operation. For the purposes of this paper, attention is focused on recent Influence Operations lead by COL Ralph Baker in selected districts of Baghdad and documented in Reference 24.

1. Framework

The selected framework for assessing Influence Operations is based on the Mission Oriented Approach to C2 assessment (Reference 12). That work was subsequently refined as the Strategies to Tasks methodology (Reference 25). The essence of those approaches is to address five inter-related questions.

- "What is the nature of the problem?"
- "What are you trying to do operationally?"
- "How are you trying to do it operationally?"
- "What gaps impede this operation in the areas of doctrine, organization, training, materiel, leadership & education, personnel, and facilities (DOTMLPF)?"
- "What steps should we take to ameliorate key DOTMLPF gaps?"

2. Nature of the Problem

To illustrate the application of the framework, COL Baker's experience in Baghdad will be assessed. For that example, COL Baker commanded the 2nd Brigade Combat Team (BCT), part of the 1st Armored Division, from 2003 to 2004. The unit was deployed in two of nine major districts in Baghdad (i.e., Karkh and Karada), covering an area of 400 km^2.

COL Baker divided the indigenous population into three categories:

- "Those who would never accept the Coalition's presence (e.g., insurgents, terrorists)";
- "Those who readily accept the Coalition's presence (e.g., secular, Western-educated pragmatists)"
- Undecided ("the vast majority").

COL Baker identified two major issues with the prior Influence Operations campaign. From a top down perspective, the activity was too slow to respond to changes on the ground and not tailored adequately to selected audiences. From a bottom up perspective, the activity was marked by inconsistent messages. COL Baker characterized the latter as "IO fratricide".

3. "What Are You Trying to Do Operationally"

COL Baker concluded that the operational goal of "winning the hearts and minds" of the populace would not be feasible. He argued that to do so would require developing

legitimate friendships. However, that would take excessive effort and time, which he lacked. Therefore, he adopted the alternative goal: “Earn the trust, confidence and respect of the Iraqis”. Consistent with that goal he pursued two themes:
• “Discredit insurgents and terrorists”;
• “Highlight economic, political, social, and security reforms”.

4. “How Are You Trying to Do It Operationally?”

COL Baker elected to reach the “undecided” population by focusing on five surrogate audiences:
• Media (focus on Arab press);
• Clerics (e.g., Imams);
• Sheiks and tribal leaders;
• Local government officials; and
• University and school leadership.

Consistent with those surrogate audiences, he employed the following key tools: psychological operations (PSYOPS); civil affairs; Public Affairs Officers (PAOs); Combat Camera; Commander’s Emergency Relief Program; and unit leaders.

He used these tools as follows. First, he modified his staff processes. This included:
• Codifying almost all Influence Operations activities in an IO Annex which was developed and issued as a fragmentary order;
• Mandating weekly or bi-weekly meetings with the leaders of the targeted audiences;
• Directing the collection of data to support weekly talking points; and
• Requiring weekly reports and monthly back-briefs.

Second, he scheduled meetings with others. This included weekly/bi-weekly meetings with surrogate audiences to listen and communicate. Furthermore, he conducted weekly roundtables with key members of the Arab press, supported by PAO activities and Iraqi “press agents”.

Finally, he implemented a sequence of feedback efforts. This included monitoring: the Arab satellite news (24 hours/day); Imam rhetoric; graffiti (noting its orientation); and the “Wave” factor (who, if any, of the Iraqi populace are waving to our soldiers).

To support these operational analyses, COL Baker used the following metrics:
- Number of accurate/positive stories published/aired;
- Lack of negative press;
- Number of walk-in or non-informant tips;
- “ Wave” factor;
- Increase/decrease of anti-US/Coalition graffiti;
- Tenor of mosque sermons; and
- Willingness of Iraqis to work with our forces.

As noted in the prior section, these metrics cut across a variety of classes of MoMs. As a strawman set, Table 4 reorganizes and augments these preliminary metrics.

Measures	Representative Measures
Functional Performance	□Time to create, validate, disseminate messages □Number of meetings held with targeted groups □Increase/decrease of anti-US/Coalition graffiti □Who is Ńwaving Ó where
Effectiveness (against targeted groups)	□Media: - Lack of negative press; - Number of accurate/positive stories published/aired □Clerics: Tone of mosque sermons
Entity Empowerment	□Improvements in economic reforms (e.g., projects completed) □Political reforms (e.g., participation in elections) □Social reforms (e.g., status of critical infrastructures) □Number, severity of insurgent, terrorist attacks (to discredit, emphasize Iraqi casualties, damage, impact)

Table 4. Strawman MoMs for Influence Operations

5. "What Gaps Impede this Operation in the Areas of DOTMLPF?"

Based on COL Baker's experience, key gaps occurred in the following areas. Doctrinally, there was a failure to be responsive and synchronized, top down and bottom up. Organizationally, COL Baker had an inadequate size and mix in his Influence Operations Working Group. From a training perspective, COL Baker had to deal with a staff that had very limited training in counter-insurgency (COIN) and media relations. From a media perspective, he lacked adequate systems to cope with shortfalls in key processes. This included a lack of automated tools to support translation of voluminous information and a lack of decision aids to support Influence Operations course of action formulation and analysis. From a leadership and education perspective, his staff lacked adequate education on cultural awareness. From a personnel perspective, he was unable to reward individuals with key skills (e.g., cultural experts). Finally, from a facilities perspective, he lacked appropriate facilities to support information sharing with the targeted audiences.

6. "What Steps should be Taken to Ameliorate Key DOTMLPF Gaps?"

In his report on his experiences (Reference 24), COL Baker identified a wide range of options to redress selected DOTMLPF gaps. The following enumeration builds upon and restructures those recommendations.

• Doctrine. First, we should reassess policies and regulations that inhibit our tactical units' ability to compete in an Influence Operations environment. Second, we should explore the potential utility of additional tools in the Influence Operations toolbox (e.g.,

computer network operations, tactical military deception). Finally, we should expand and restructure the family of MoMs to facilitate the implementation and analysis of Influence Operations.
• Organization. Based on COL Baker's experiences, we should rethink the size and composition of the Influence Operations Working Group (e.g., use of Intelligence personnel to support Public Affairs).
• Training. COL Baker formulated two recommendations that are currently being partially implemented. We must require COIN instruction at all levels in our institutional training base and we must increase the quality and quantity of media training provided to Soldiers.
• Materiel. We should expedite the development, transition, and use of automated translation devices (both written and spoken) from DARPA to the Army and Marine Corps. Furthermore, we should expedite the Information Operations Joint Munitions Effects Manual (JMEM) activities to develop and field decision aids to support Influence Operations course of action analysis.
• Leadership and Education. Consistent with the recommendations of COL Baker, we should increase the quality and quantity of media training provided to Service leaders and integrate cultural awareness education as a standard component in our institutional curriculum.
• Personnel. As recommended by COL Baker, we should consider compensating culture experts, commensurate with their expertise.
• Facilities. Currently, there are many facilities to enhance information sharing in the area of operations (AOR). We should standardize and populate Civil-Military Operations Centers (CMOCs) to facilitate information sharing with non-military participants. These facilities should emphasize sharing information in cyberspace to minimize face-to-face physical interactions and enable these participants to be perceived as un-biased.

7. Summary

The proposed mission oriented framework provides a logical way of organizing and addressing Influence Operations issues. Furthermore, the DOTMLPF paradigm provides a systematic means of identifying gaps and formulating holistic packages of actions to redress those gaps.

E. OBSERVATIONS

Based on these preliminary analyses, some broad observations about cyberpower and residual issues are emerging. At layer 1 of the pyramid ("Cyber-Infrastructure"), it is clear that conflict in cyberspace differs from conflict in physical space in several key ways. First, cyberspace is a man-made environment that is experiencing exponential change. Although we have some indications about key trends, it is not possible to predict its MoPs, reliably, over the next fifteen years. In particular, there is profound concern that the erosion of security in cyberspace will adversely affect key levers of power (e.g., military, economic). This suggests that a new cyberspace architecture may be required that diverges from the current Internet architecture. If this new, more robust architecture does emerge (e.g., through NSF's FIND or DARPA's AGN), it will pose major challenges in transitioning from the current legacy architecture. In addition, there is

extraordinary diffusion of information about cyberspace among key stakeholders. Thus, no single user will be able to achieve and retain a monopoly of knowledge of cyberspace.

At layer 2 of the pyramid ("Levers of Power"), the military user must confront the implications of uncertain security. These concerns are highlighted by daily events that are headlined in the media (e.g., the Chinese test of an anti-satellite device (Reference 26); or the attack of the Domain Name Server (DNS) system by hackers (Reference 27)). As one response, the military Services are proceeding to create and field a Cybercorps (Reference 28). However, it is still unclear what role such an organization might play. More broadly, the US Government must explore the broader role that cyberspace may play in SRO. As an example, the recent paper on I-Power (Reference 23) suggests that information and communications technology could be a significant enabler of reconstruction operations in other key sectors (e.g., education, health care).

At layer 3 of the pyramid ("Empowerment"), it is becoming clear that there is an unintended consequence of changes in cyberspace: life is becoming more dangerous for industrialized nations and their populations. This is a direct consequence of the increased power that terrorists and transnational criminals are deriving from innovative applications of cyberspace. This is due, in part, to the empowerment that the private sector is deriving from the use of cyberspace. Exploitation of cyberspace is incredibly important to the private sector and its importance is continuing to grow. This has spawned reduced costs and enhanced capabilities for cyberspace transport, services, and applications that provide a (nearly) "free-ride" for terrorists and transnational criminals. In addition, it is uncertain how other nation states (e.g., China, Russia) may evolve their use of cyberspace to enhance their power at the expense of Western nations.

In the other facet of the pyramid ("Institutional Issues"), it is becoming clear that there is a need to pay more attention to governance and legal issues, over a strategic planning horizon. Current decisions are being made tactically, and there is little understanding about their long-term ramifications on cyberpower. Ultimately, there are profound issues to address over the role that the US government will play. There are suggestions that it should formulate requirements and provide incentives and disincentives for the stakeholders in cyberspace. However, it is unclear about the resources that the US government should invest in the critical area of cyberspace research.

F. REFERENCES

1. 2006 Quadrennial Defense Review, Office of the secretary of Defense, 6 February 2006.
2. Dan Kuehl, "Cyberspace and Cyberpower: Their Influence on (Future) History", Chapter in "A Theory of Cyberpower", CTNSP, NDU, to be published in Fall 2007.
3. Ed Skoudis, "Evolutionary Trends in Cyberspace", Ibid.
4. Elihu Zimet, "Elements of Cyberspace", Ibid.
5. Marjorie S. Blumenthal and David D. Clark, "Bounding the Future of the Internet", Ibid.
6. Greg Rattray, "Understanding Cyberpower", Ibid.

7. Martin Libicki, “Military Cyberpower: The Case of Tactical Ground and Air Network-Centric Operations”, Ibid.
8. Daniel Gonzales, et al, “Network-Centric Operations Case Study: Air-to-Air Combat With and Without Link 16”, RAND, National Defense Research Institute, 2005.
9. Daniel Gonzales, et al,“ Network-Centric Operations Case Study: The Stryker Brigade Combat Team”, RAND, National Defense Research Institute, 2005.
10. Franklin Kramer and Larry Wentz, “Cyber Influence Operations in International Contexts”, Chapter in “A Theory of Cyberpower”, CTNSP, NDU, to be published in Fall 2007.
11. Stuart H. Star, “A Framework for Influence Operations and A Tactical Example”, Ibid.
12. David T. Signori and Stuart H. Starr, “The Mission Oriented Approach to NATO C2 Planning”, Signal Magazine, pp 119 – 127, September 1987.
13. Jarret Brachman, “How Terrorists Are Empowered by Cyberspace”, Chapter in “A Theory of Cyberpower”, CTNSP, NDU, to be published in Fall 2007.
14. Kevin Burton, “How Transnational Criminals Are Empowered by Cyberspace”, Ibid.
15. Tim Thomas, “How Nation States Are Empowered by Cyberspace”, Ibid.
16. Harold Kwalwasser, “Governance of Cyberspace”, Ibid.
17. Will O’Neil, “Critical Infrastructure Protection and Cyberspace”, Ibid.
18. Tom Wingfield, “Legal Issues and Cyberspace”, Ibid.
19. Jim Kadtke, “Preliminary Perspectives on Methods and Tools to Analyze Key Cyberpower Issues”, Ibid.
20. “NATO Code of Best Practice for C2 Assessment”, reprinted by Command and Control Research Program (CCRP), OSD, revised 2002.
21. John Soat, “IT Confidential: Is There Anything That Can Be Done About E-mail?”, Information Week, February 17, 2007.
22. Deputy Secretary of Defense, DoD Directive 8320.2, “Data sharing in a Net-Centric DoD”, Modified January 26, 2007.
23. Franklin D. Kramer, Larry Wentz, and Stuart Starr, “I-Power: The Information Revolution and Stability Operations”, Defense Horizons, Number 55, CTNSP, NDU, February 2007.
24. COL Ralph Baker, “The Decisive Weapon: A Brigade Combat Team Commander’s Perspective on Information Operations”, Military Review, May-June 2006.
25. Leslie Lewis, et al, “Defining a Common Planning Framework for the Air Force”, RAND, ISBN 0-8330-2730-1, 1999.
26. Bill Gertz, “China Has Gained and Tested Array of Space Weapons”, Washington Times, p. 8, March 30, 2007.
27. ICANN, Factsheet, “Root server attack on 6 February, 2007”, 1 March 2007.
28. Derek Gabbard, Chris May, and Jeff Thieret, “Air Force CyberCorps: Recruit, Organize, Train, and Retain”, CERT, Systems Engineering Institute, Pittsburg, PA, July 7, 2006.

G. AUTHORS

Franklin D. Kramer is a Distinguished Research Fellow at CTNSP, NDU. He served as the Assistant Secretary of Defense (International Security Affairs) from 1996 to 2001.

Daniel Kuehl is a Professor at the Information Resource Management College, NDU.

Stuart H. Starr is a Senior Research Fellow at CTNSP, NDU. He served as the Director of Plans at the MITRE Corporation and is a member of the Army Science Board.

Larry Wentz is a Senior Research Fellow at CTNSP, NDU. He served as Technical Director for Joint and Defense-Wide C3 at the MITRE Corporation.

Elihu Zimet is a Distinguished Research Fellow at CTNSP, NDU. He served as the Head, Expeditionary Warfare Department, Office of Naval Research, and is a member of the Naval Studies Board.

Towards a Theory of Cyberpower

Franklin Kramer, Stuart Starr, Larry Wentz, Eli Zimet
CTNSP, NDU
Dan Kuehl
IRMC, NDU

June, 2007

Agenda

- Context
- Goal, Objectives
- Framework
- Selected Observations
- Summary

“For Estonia and NATO, A New Kind of War”*

- What/When
  - Cyberspace attacks against Estonia (presumably by Russia)
  - Spring 2007
- Key Questions
  - Is this an “armed attack”?
  - Is the NATO alliance obliged to respond?
  - And if yes, how?

* Anne Applebaum, Washington Post, May 22, 2007

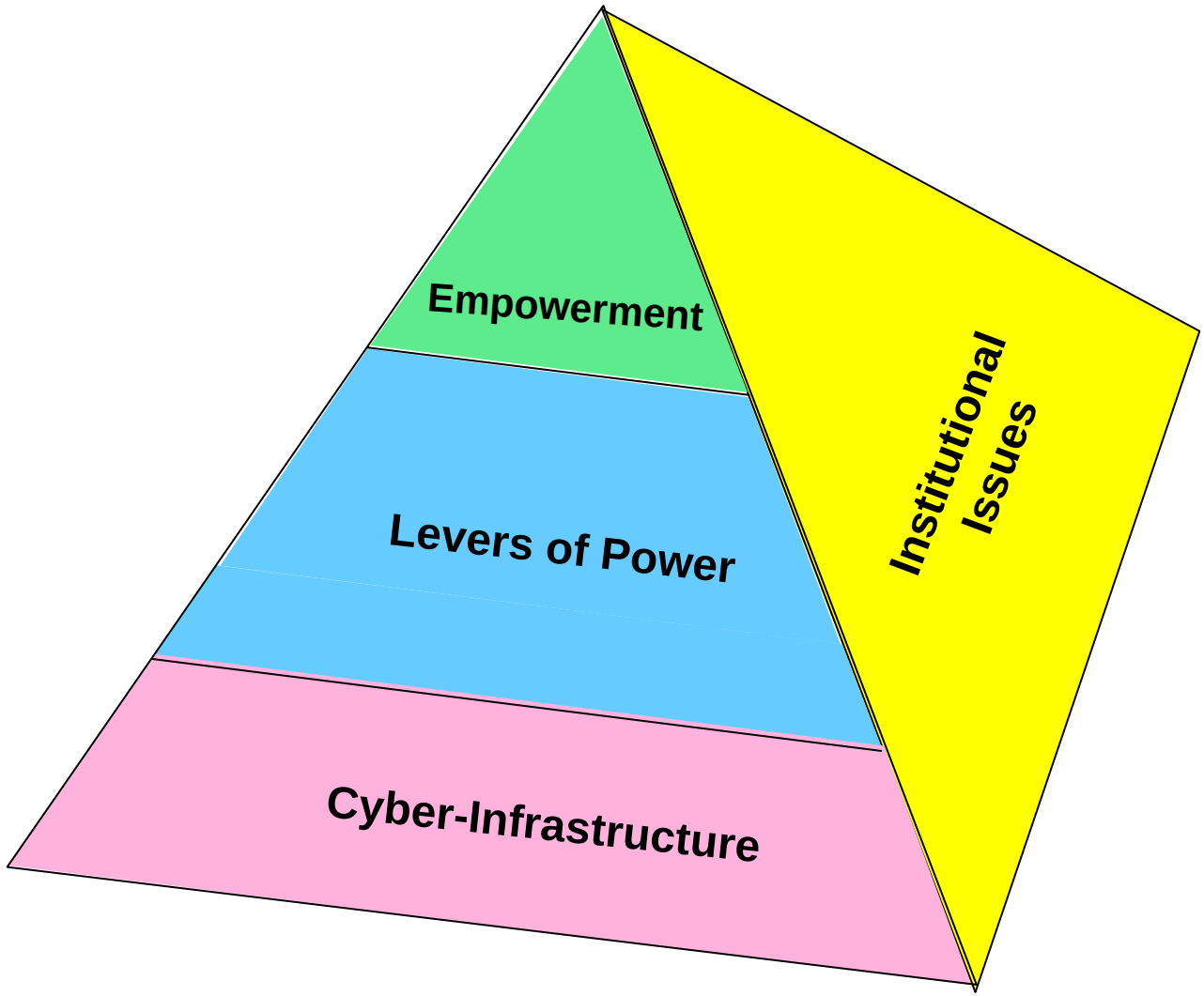
Goal

- "… there is a compelling need for a **comprehensive, robust and articulate cyber power theory** that describes, explains and predicts how our nation should best use cyber power in support of US national and security interests"
- "The theory should account for
  - The nation's increased use of and reliance upon national security, civil and commercial cyber capabilities
  - Other nations' and non-governmental actors' use of cyberspace
  - Direct challenges to the US's use of cyberspace
  - The changed and projected geo-strategic environment"

Objectives

- From a national security perspective, provide **frameworks** to structure cyberpower issues
- Identify and characterize major **cyberpower issues**
- Identify and explore **methods and tools** to perform policy analyses of cyberpower issues

Framework

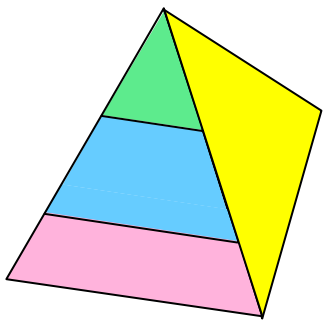

Empowerment
Levers of Power
Cyber-Infrastructure
Institutional Issues

Key Definitions

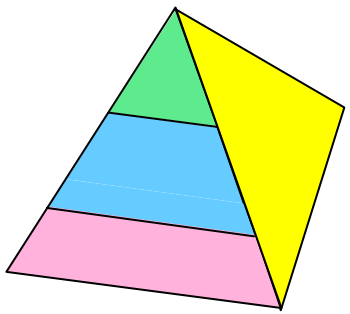
- "**Cyberspace** is an operational domain characterized by the use of electronics and the electronic spectrum to create, store, modify, and exchange information via networked and interconnected information systems and telematic infrastructures."
- " **Cyberpower** is the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power."
- "**Cyberstrategy** is the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power."

Key Activities: Cyber-Infrastructure

- Dan Kuehl, “Cyberspace, Cyberpower, Cyberstrategy”
- Eli Zimet, “Domains of Cyberspace”
- Ed Skoudis,
  - “Evolutionary Trends in Cyberspace”
  - “Security in Cyberspace”
- Marjorie Blumenthal, Dave Clark, “Revolutionary Trends in Cyberspace”
- Will O’Neil, “Critical Infrastructure Protection (CIP)”



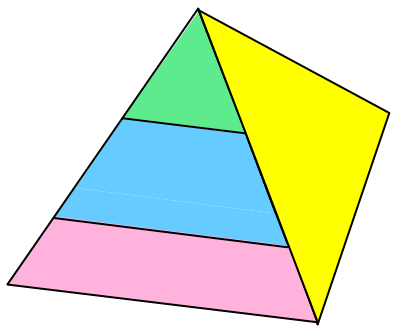
Key Activities: Levers of Power



- Greg Rattray,
  - "Principles of Cyberpower"
  - "Military Benefits & Risks in Cyberspace"
- Martin Libicki, "Military Applications of Cyberspace"
- Service perspectives on cyberspace
- Frank Kramer, Larry Wentz, "Influence Operations: Strategic and Operational Perspectives"
- Stuart Starr, "Influence Operations: Tactical Perspectives"

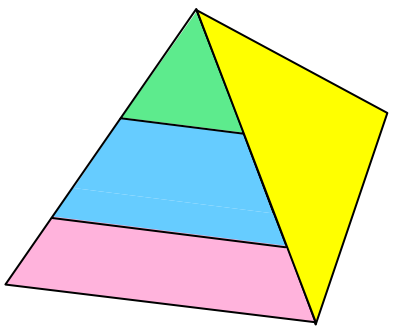
Key Activities: Empowerment

- Jarret Brachman, “Empowerment of Terrorists by Cyberspace”
- Eric Burton, Clay Wilson, “Empowerment of Transnational Criminals by Cyberspace”
- Tim Thomas, “Empowerment of Nation States by Cyberspace”
- Dick Kugler, “Deterrence in Cyberspace”



Key Activities: Institutional Issues

- Hal Kwalwasser, “Governance in Cyberspace”
- Tom Wingfield, “Legal Perspectives on Cyberspace”
- John McCarthy, “Institutional Aspects of CIP”
- Jim Kadtke, “Methods & Tools to Address Cyberpower Issues”



Military Opportunities & Risks in Cyberspace

Level	Opportunities	Risks
Strategic	• NCW-enabled • New “Center of Gravity” opportunities (e.g., deterrence; “virtual conflict”)	• Loss of technical advantage • Rapidly changing operating environment • Military dependence on key systems (e.g., GIG)
Operational	• Phasing of operations • Enhanced force structure mix (e.g., cheaper, more precise)	• Loss of advantage in operational pace
Tactical	• Discover and track adversaries using cyberspace	• New front for adversaries to build resources

We are assuming significant, unknown risk

Options to Address Military Cyberspace Issues

Strategic	Ensure resilience of supporting infrastructures
Operational	Plan to conduct operations against an adversary that is highly cyberwar-capable
Programs	Address cyberspace implications in the development process (e.g., Information Assurance)

Improve analytic capability

Summary (1 of 2)

- Cyber-Infrastructure
  - Cyberspace is a man-made environment that is experiencing
    - Exponential growth
    - Extraordinary diffusion of knowledge among stakeholders
  - The erosion of security in cyberspace is likely to adversely affect key levers of power
  - A new cyberspace architecture may be required to halt this erosion of security
- Levers of Power
  - The military must confront the implications of uncertain security to address unknown risks
  - Cyberspace has the potential to play an increasingly important role in stabilization and reconstruction operations (“I-Power”)

Summary (2 of 2)

- Empowerment
  - Changes in cyberspace have given rise to unintended consequences – it is making life more dangerous for information-enabled societies (e.g., enhanced power of terrorists, transnational criminals)
  - It is uncertain how near-peers (e.g., China, Russia) will exploit cyberpower
  - There is a need for “tailored deterrence” in cyberspace
- Institutional
  - Additional attention must be paid to key cyberspace issues (e.g., governance, legal, government-corporate responsibilities)
  - Research efforts are required to develop methods and tools to address cyberspace policy issues